Appeal No: 24-3161

IN THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

ROMAN STERLINGOV,

Appellant

v.

UNITED STATES OF AMERICA,

Appellee

On Appeal from United States District Court for the District of Columbia Hon. Randolph D. Moss United States District Court Case No. 1-21-cr-00399-RDM-1

BRIEF OF AMICUS CURIAE CHAINARGOS IN SUPPORT OF APPELLANT ROMAN STERLINGOV'S APPEAL & REVERSAL OF CONVICTION

(All Parties Have Consented to Filing)

September 22, 2025

Joseph A. Scrofano
Scrofano Law PC
D.C. Cir. Bar No: 60117
600 F St NW Suite 300
Washington, DC 20004
(202) 870-0889
jas@scrofanolaw.com

Counsel for Amicus Curiae ChainArgos

TABLE OF CONTENTS

TABLE OF AUTHORITIES

OTHER AUTHORITIES

S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, Dec 2008.....15

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1 and D.C. Cir. Rule 26.1, ChainArgos PTE. Ltd. [hereinafter "ChainArgos"] states that it has no parent corporation and no publicly held corporation owns 10% or more of its stock.

CONSENT

Counsel for Appellant Roman Sterlingov has consented to the filing of this brief. Counsel for Appellee United States has also consented. Therefore, all parties consent to the filing of this brief.

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES,

Pursuant to D.C. Circuit Rules 28(a)(1) and 32.1, counsel for ChainArgos states as follows:

Parties and Amicus

The parties appearing before the District Court and all persons who are parties before this Court are as follows:

Appellant - Roman Sterlingov

Appellee - The United States of America

Amicus - ChainArgos

Rulings under Review

This appeal arises from the judgment in a criminal case entered by the U.S. District Court for the District of Columbia on November 13, 2024, in Case No. 1:21-CR-00399.1 Sterlingov appeals, as argued below, the District Court's:

- Denial of his Motion to dismiss filed August 1, 2022, and denied orally from the bench at trial on February 13, 2024, particularly as to venue and the statute of limitations, as well as the Jury Charge on venue in relation to Count One

- Pretrial and trial oral and written admission of Government expert witness testimony under *Daubert*

- Denial of Appellant's access to the Chainalysis Reactor closed source code, as well as full access to Reactor's proprietary heuristics

- Admission of irrelevant and highly prejudicial evidence of child pornography

- Issuance, over objection, of a willful blindness jury instruction

- Denial of Appellant's oral motions for a judgment of acquittal at the close of the Government's and Appellant's case in chief

- Admission, over objection, of irrelevant, highly prejudicial testimony from cooperating Government criminal witnesses Illya Lichtentstein and Larry Harmon

- Provisional admission of co-conspirator hearsay statements without foundation and without any fact finding when it permanently admitted the statements into evidence.

- Miscalculation of the "Value of the Laundered Funds" Under U.S.S.G. § 2S1.1(a)(2)

Related Cases

The case under review was not before this Court or any other court, other than the District Court from which it is appealed and the District Court in the Central District of California where Defendant was originally detained and arraigned.

RULE 29(a)(4)(E) STATEMENT

Amicus states that (i) a party's counsel has not authored the brief in whole or in part; (ii) a party or a party's counsel has not contributed money that was intended to fund preparing or submitting the brief; and (iii) no person—other than the amicus curiae, its members, or its counsel—contributed money that was intended to fund preparing or submitting the brief.

STATEMENT OF AMICUS CURIAE

ChainArgos is a Singapore-based specialist blockchain intelligence firm, that provides blockchain data and analytics software, as well as expert witness testimony and litigation consulting on a variety of crypto-asset and blockchain-related legal matters. Our mission is to provide blockchain intelligence solutions in service of the truth, founded on principles of mathematics, statistics, and forensic science, and delivering actionable insight into blockchain transaction data that is both accurate, and independently verifiable. The rapid growth of crypto-assets and blockchain technology has resulted in the birth of blockchain tracing as a cottage industry. However, the blockchain analysis industry and its methodologies have not been subject to scientific or statistical testing, with subjective outcomes putting innocent people at risk of being deprived of their constitutional rights based on nothing more than pseudo-science and conjecture, masquerading as a technological solution.

ChainArgos believes Americans should be free to transact on the blockchain without fear of unverified blockchain tracing methodologies hanging over their heads like the Sword of Damocles, undermining the American lead in

crypto-assets and blockchain technology. ChainArgos is arguing that the government experts' blockchain tracing used to convict the Appellant in the District Court was fundamentally flawed, rendering the results derived entirely unreliable and ought to have been ruled inadmissible, violates the Fifth Amendment, and is unconstitutional.

ARGUMENT

The government's conviction of the Appellant relies upon fundamentally flawed blockchain tracing methodologies that are demonstrably unreliable and should have been inadmissible under the rigorous standards required by the Court. To assist this Court, ChainArgos will begin by thoroughly dissecting the technical and scientific deficiencies of the government expert's attribution methods, address the significant inaccuracies in its assessment of Bitcoin Fog's impact, present empirical evidence regarding CoinJoins, and finally, highlight the critical errors in applying their blockchain tracing to the facts at issue in this case.

ChainArgos do not claim the government's, or the government's contracts, tools and methods are useless or fraudulent. Rather, ChainArgos believes the government's claims of accuracy and reliability have been dramatically overstated, are fundamentally unscientific, and inconsistent with what it has witnessed in practice. ChainArgues argues using publicly available blockchain transaction data, and public statements by the government's own experts demonstrates this.

I. The Government Experts' Attribution Methodology

The government's primary method for attributing blockchain transactions relies on heuristics that are both flawed and unreliable, failing to meet the standards for forensic evidence and admissibility. A "heuristic" is another word for a "guess" and in certain circumstances it can also be construed as an "educated guess" and is a necessary step in the experimentation process, insofar as such process can be subject to testing. However, when claims are made that a "heuristic" is inherently reliable without providing any independent proof that such reliability has been tested, then it is only reasonable that such a "heuristic" must be called into question.

A. The "Co-Spend" Heuristic is Flawed and Unreliable

The government's expert, Luke Scholl, testified that the "co-spending" heuristic was the "primary heuristic" used by Chainalysis Reactor.[1] This heuristic, as described by Meiklejohn et al.[2] ("Meiklejohn Paper"), suggests that "the sender in the transaction *must* know the private signing key belonging to each public key used as an input, so it is unlikely that the collection of public keys are controlled by multiple entities" (emphasis added).

However, this assertion is both inaccurate and unsubstantiated. While the Meiklejohn Paper notes that such algorithms, similar to those relied upon by Ron

---

[1] Scholl, *Daubert* Hearing, June 23, 2023, at 77:13; Appx. 577.

[2] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage. A fistful of bitcoins: characterizing payments among men with no names. Commun. ACM, 59(4):86–93, Mar 2016. ISSN 0001-0782. DOI: 10.1145/2896384. URL https://doi.org/10.1145/2896384

and Shamir,[3] can lead to "overestimation errors" (associating clusters of blockchain addresses with the same person without justification), this is precisely the type of error to which the "co-spending" heuristic is particularly susceptible. The Meiklejohn Paper's predicate assumption that "the sender in the transaction must know that private signing key belonging to each public key used as an input" is not merely untrue, it is also taken entirely out of context and elevated to an axiom in a manner wholly inconsistent with accepted standards of forensic evidence admissible in court.

Twenty-five years even before Bitcoin was created, it had already been demonstrated that[4] participants in a CoinJoin[5] do not in fact need to share private keys, directly contradicting the government expert's core allegation. While it is true, as per the Meiklejohn Paper, that the private keys of all the participants in a Coinjoin must be entered into the transaction via a process, computer scientists have known since 1983 that this process does not necessarily require the senders to exchange this private key information amongst themselves because there are

---

[3] D. Ron and A. Shamir. Quantitative analysis of the full bitcoin transaction graph. In A.-R. Sadeghi, editor, Financial Cryptography and Data Security, pages 6-24, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. ISBN 978-3-642-39884-1.

[4] D. Chaum. Blind signatures for untraceable payments. In D. Chaum, R. L. Rivest, and A. T. Sherman, editors, Advances in Cryptology, pages 199–203, Boston, MA, 1983. Springer US. ISBN 978-1-4757-0602-4.

[5] CoinJoins are single bitcoin transactions with multiple inputs and outputs and pose a significant challenge to blockchain analysis. Coinjoins, in the most basic sense, are straightforward to detect in public transaction data. If a given transaction has two or more inputs and two or more outputs that is treated as a CoinJoin. This is a slightly more expansive definition of a CoinJoin than adopted by other studies but the definition weathers well under scrutiny when held up against the empirical transaction data.

other methods by which to coordinate such a Coinjoin without the sharing of private keys.

In fact, Jonathan Levin, a co-founder of Chainalysis Inc., which developed the Chainalysis Reactor software used by the government, has himself acknowledged the limitations of the "co-spending" heuristic, especially in the context of CoinJoins in a paper entitled "Tracking Ransomware End-to-end" ("the Ransomware Paper")[6]:

> We stress that the clustering technique does not apply to CoinJoin transactions, which violate the co-spending heuristic. The sender of a CoinJoin transaction does not have access to the private keys of the input wallet addresses. Effectively, two addresses that are co-spent in the same CoinJoin transaction cannot be clustered together. To detect CoinJoin transactions in our clustering, we apply a set of heuristics[7] using BlockSci.[8] We find no CoinJoin transactions in our clusters, although there is still a possibility that the heuristics might have failed to detect some CoinJoin transactions. We will mitigate this problem in Section IV-F by proposing and evaluating filtering techniques.

The assertion by Levin et al. that they "found no CoinJoin transactions in our clusters" and thus no reason to doubt their methods does not make their methods "unquestionably flawless". This perspective is not just an affront to "Schneier's Law,"[9] a known adage in computer science which states that "any

---

[6] URL https://ieeexplore.ieee.org/document/8418627
[7] S. Goldfeder, H. A. Kalodner, D. Reisman, and A. Narayanan. When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. CoRR, abs/1708.04748, 2017. URL http://arxiv.org/abs/1708.04748
[8] H. Kalodner, S. Goldfeder, A. Chator, M. Moser, and A. Narayanan. Blocksci: Design and applications of a blockchain analysis platform. URL https://www.usenix.org/conference/usenixsecurity20/presentation/kalodner
[9] B. Schneier. Schneier's law, 2011. URL https://www.schneier.com/blog/archives/2011/04/schneiers_law.html.

person can invent a security system so clever they cannot think of how to break it", assuming a detection technique is reliable simply because its creators have not identified its vulnerabilities is fundamentally unscientific.

The first known mixing service on the Bitcoin blockchain that did not require sharing private keys was launched in 2013,[10] and CoinJoins were rampant on the Bitcoin blockchain for years prior to that.[11] Yet, the government's expert, Luke Scholl ("Scholl"), was unable to cite any scientific peer-reviewed paper addressing the accuracy of Chainalysis Reactor's detection of CoinJoins in a "co-spending" heuristic.[12] Instead, both Scholl and the authors of the Ransomware Paper relied on a "proprietary heuristics-based algorithm" whose details remain opaque[13]:

> Chainalysis is a proprietary online service that links clusters of wallet addresses to the likely real-world identities. It regularly transacts with known Bitcoin-related services, such as exchanges, to discover and cluster wallet addresses used by these services, while excluding CoinJoin transactions using a proprietary heuristics-based algorithm.

This statement attempts to define the problem but fails to address the persistent issue of CoinJoins, which were highly prevalent even in the early years of the Bitcoin blockchain. Without further information about this "proprietary

---

[10] G. Maxwell. Coinjoin: Bitcoin privacy for the real world. In Post on Bitcoin forum, volume 3, page 110, 2013.
[11] J. Reiter. An empirical study of early coinjoins: Placing limits on blockchain tracing in the early years of bitcoin, 2024.
[12] Scholl, *Daubert* Hearing, June 23, 2023, at 79:18-22; Appx. 579.
[13] *Supra*, note 6 at page 625.

online service," we are left with Chainalysis' reference to BlockSci's heuristics, which states[14]:

> Two common types of heuristics include (1) inputs spent in the same transaction are controlled by the same entity, and (2) identifying a change address based on client software or user behavior. As the multi-input heuristic does not apply to CoinJoin transactions, we add an exception for those transactions, which we identify using the algorithm described by Goldfeder et al.

Goldfeder et al. refer to their algorithm as a method to "deanonymize users of cryptocurrencies" through "third-party web trackers"[15]. However, at the time of the transactions relevant to the Appellant, web-browser add-ons for Bitcoin wallets were not in widespread use, casting doubt on the applicability of this method to these specific transactions.

Crucially, none of the heuristics relied on by the government have been tested to even the most minimum standards required for forensic science, yet the District Court was unreasonably asked to determine the reliability and admissibility of the government's blockchain analysis.

The United States National Academy of Sciences, in a landmark report[16] to Congress ("USNAS Report"), directly addresses such forensic issues, emphasizing that lawyers and judges are often unreasonably held to determine the reliability of forensic evidence, without being equipped with the necessary

---

[14] *Supra*, note 8 at page 2725.
[15] *Supra*, note 7 at page 5.
[16] National Research Council. Strengthening forensic science in the United States: A path forward, 2009. URL http://www.nap.edu/catalog/12589.html.

scientific methodologies to do so. The USNAS Report, compiled by distinguished researchers and legal experts including several federal judges and law professors, clearly states that conformance with a "checklist" does not guarantee reliability, which for all intents and purposes, is all the government's expert witness provided in its blockchain tracing.

In conclusion, the "co-spend" heuristic, particularly given the prevalence of CoinJoins, is unreliable at best. In line with the USNAS Report, and basic scientific principles, these techniques should be presumed unreliable absent evidence of reliability. As ChainArgos discusses later, anecdotal evidence that these techniques can generate useful investigative leads should not be conflated with evidence these techniques can reliably identify blockchain address owners in all circumstances.

The government may have relied on commercial blockchain tracing services that identified actors in the proximity of illicit bitcoin transactions, but a central goal of all legal systems is to convict individuals for crimes they actually committed, not ones they were proximate to. This distinction is precisely the risk created by applying the "co-spend" heuristic without any data assessing its reliability and why the admission of such evidence is in violation of the Appellant's Fifth Amendment rights.

B. Comparison of Blockchain Analysis with Other Forms of Evidence

When evaluating any blockchain tracing or attribution methodology, especially when it is being relied on in a criminal conviction, it is appropriate to

compare it against the highest standards of attribution, such as DNA evidence. Both blockchain analysis and DNA evidence involve complex "lab" techniques rooted in mathematics. However, forensic methods have developed useful standards that not only provide actionable insights but also effectively manage false positives. All lab techniques are prone to error and more broadly: all investigative techniques are prone to error. Acknowledging, studying and managing those errors forms a core part of the legal processes around forensic evidence.

The USNAS Report highlights that, with the exception of nuclear DNA analysis, "no forensic method has been rigorously shown to have the capacity to consistently, and with a high degree of certainty, demonstrate a connection between evidence and a specific individual or source". Blockchain tracing, absent additional corroborating evidence, generally cannot provide a degree of certainty even remotely close to DNA evidence.

Furthermore, while some components of blockchain tracing are exceptionally difficult to falsify (e.g., the certainty that the same private key was used for two transactions from the same source wallet address), others are trivial to manipulate. For example, anyone can transfer their private keys to a bitcoin wallet address discreetly and in person, without reliance on a public blockchain transaction, whereas altering one's DNA poses significantly more challenges. Fingerprint matches, by comparison, are graded on a scale with established thresholds, acknowledging that perfect matches are not always required. This

demonstrates the need for a body of research to determine the conclusiveness of any analysis, not just blockchain tracing. When fingerprint analysis was first employed, a grading system and framework for evaluating matches did not exist. That framework evolved gradually over time to manage the uncertainty and inevitably error-prone practices around the core technique.

In the context of Bitcoin, a private key either works or it does not; there are no "intermediate levels of access," nor is there a "6-point" match for a Bitcoin wallet's private key. Blockchain analysis is unique in that it is entirely possible to effect undetectable ownership changes of crypto-asset wallet addresses. Assuming such ownership changes never occur, without understanding their prevalence, is entirely unjustified and unjustifiable.

Other researchers have analyzed the design and effectiveness of blockchain tracing relying on the "co-spending" heuristic. Even when limited to specific CoinJoin packages following "intricate" research, these researchers found significant levels of uncertainty in analyzing public blockchain records within highly controlled study environments.[17] Broader studies[18] of general wallet clustering heuristics to determine "cluster effectiveness" (related to, but not equivalent to, accuracy) generally achieved only 95% to 98% coverage of clusters, without even attempting to measure error rates. This means 2% to 5% of

[17] H. Schnoering and M. Vazirgiannis. Heuristics for detecting coinjoin transactions on the bitcoin blockchain, 2023.
[18] H. Schnoering, P. Porthaux, and M. Vazirgiannis. Assessing the efficacy of heuristic-based address clustering for bitcoin, 2024.

samples could not be classified, a level inferior even to contactless fingerprint matching[19] where a recent NIST study[20] found that:

> this early study finds contactless fingerprints of the devices examined to be useable in some applications, with qualifications...users should expect larger error rates with machine matching and difficulty with any forensic applications such as latent matching, or support of courtroom testimony.

If these wallet clustering techniques are inferior to contactless fingerprinting, then they are, quite literally, worse than a technique where NIST said "users should expect...difficulty with...support of courtroom testimony." Amicus' position is that NIST is correct and this testimony should never have been presented to a jury.

C. Unreliability of Behavioral Analysis

The government's expert Scholl, also testified about a "behavioral heuristic" used in their blockchain analysis, described as[21]:

> the behavioral heuristic is based off the way that the transactions occur and the digital fingerprints that are left behind from the interaction of a wallet software. So that is provable because it's done and replicated time and time again and very reliable.

However, the same expert conceded that no academic studies of this analysis have been conducted, nor has there been any independent assessment of the integrity of this "behavioral heuristic". The expert's reference to "digital

---

[19] J. Libert, J. Grantham, B. Bandini, K. Ko, S. Orandi, and C. Watson. Interoperability assessment 2019: Contactless-to-contact fingerprint capture, 2020-05-19 2020.
[20]NIST, Guidance for Evaluating Contactless Fingerprint Acquisition Devices, 2018, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-305.pdf
[21] Scholl, *Daubert* Hearing, June 23, 2023, at 127:17-21; Appx. 627.

fingerprints" left by wallet software creates the misconception that the Bitcoin blockchain can only be interacted with using "wallet software". In reality, anyone can write their own transaction-signing program for the Bitcoin blockchain, and guides are readily available online for this purpose, none of which require any exceptional programming skills.

It is plausible that individuals with the ability to write such programs could mimic or randomly alter "digital fingerprints" to increase the level of obfuscation for their Bitcoin transactions. Given that many commonly used wallet software packages are open-source, it is even more plausible that someone with rudimentary programming skills could combine several wallet software programs into a "meta wallet" that randomly alters the "digital fingerprint" for each transaction.

Without empirical and thorough analysis of "digital fingerprints" in the context of the government expert's "behavioral heuristic", and without any data or understanding of its susceptibility to attack, how can such a methodology be determined to be "very reliable" when it has never been tested or subject to scrutiny? Such claims are fundamentally unscientific and, in line with the USNAS Report, these sorts of forensic techniques have no place in a courtroom until a more solid foundation for their admissibility is established.

II. Flaws in the Government's Empirical Analysis of CoinJoins.

The government's expert analysis fundamentally neglects the overwhelming prevalence and characteristics of CoinJoins on the Bitcoin blockchain, especially during the period in question in this case.

D. The Government's Inadequate Definition of a CoinJoin

CoinJoins, which are single bitcoin transactions with multiple inputs and multiple outputs, present a significant challenge to blockchain tracing. In the most basic sense, CoinJoins are straightforward to detect in public transaction data: any transaction with two or more inputs and two or more outputs can be treated as a CoinJoin. While this definition may be slightly more expansive than other studies, it withstands scrutiny when compared against empirical transaction data.

Even a CoinJoin with only two inputs and two outputs ("2X2") provides a limited level of obfuscation in a single transaction. However, it is entirely possible to run multiple rounds of CoinJoins, even with initial 2X2 transactions. Given that transaction fees were exceptionally low in dollar terms during the early years of the Bitcoin blockchain, it is highly improbable that bitcoin users would have traded efficiency for privacy, especially considering the libertarian roots of the Bitcoin blockchain. Indeed, empirical evidence confirms the widespread use of CoinJoins and other obfuscation techniques within months of the Bitcoin blockchain's inception.[22]

E. Identifying Large Bitcoin Transactions is Not Proof of Reliability of Tracing

---

[22] *Supra*, note 11**Error! Unknown switch argument.**.

Blockchain tracing demonstrates some reliability when applied to the movement of transactions hundreds or thousands of times the average size for a given period. In such rare situations, the set of plausible routes for a Bitcoin transaction is exceptionally limited, and if a single plausible route exists, it can be accurately traced independent of specific heuristics, whether proprietary or otherwise, often through exhaustive search algorithms.

However, blockchain tracing struggles profoundly when the quantum of bitcoin transacted is not statistically larger than the average and is otherwise indistinguishable from the vast majority of transactions on the Bitcoin blockchain. In these common situations, a large number of plausible routes exist for any given Bitcoin transaction, and without relevant external information to corroborate attribution, the value of blockchain tracing is, at best, extremely limited. This does not mean blockchain tracing is entirely without value, because identifying a set of plausible transaction pathways for further investigation is useful for preliminary investigations, but using such analysis to determine culpability would be wholly disproportionate to its evidentiary value.

F. Bitcoin Transaction Best Practices Recommend Obfuscation

Despite the government's assertions, Bitcoin transaction best practices, from its very inception, have encouraged obfuscation and privacy, not transparency. Although a Bitcoin transaction *can* use the same input and output address, the

recommended best practice from the outset was to avoid reusing addresses. As Satoshi Nakamoto himself wrote in the Bitcoin whitepaper[23]:

As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner.

This recommendation, advising users of the Bitcoin blockchain not to reuse addresses, was widely adopted, as clearly visible in Figure 2 of APPENDIX A. The practice of using fresh Bitcoin blockchain addresses in transactions began in 2009, coinciding with an increase in Bitcoin transaction volumes, even before well-known obfuscation services were widely operational.

Nakamoto also explicitly highlighted the vulnerability of multi-input Bitcoin transactions to the "co-spend heuristic," warning:

> Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner.

Knowing this, early bitcoin users swiftly adapted, employing methods specifically designed to overcome this vulnerability.

G. Analysis of CoinJoins and Bitcoin Fog

The government has made public a large number of Bitcoin blockchain addresses it alleges belong to Bitcoin Fog ("Bitcoin Fog Addresses"). An analysis of CoinJoins involving these Bitcoin Fog Addresses by month, as provided in Figure 3 of APPENDIX A, reveals that these addresses were already involved in

---

[23] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, Dec 2008. URL https://bitcoin.org/bitcoin.pdf

thousands of CoinJoins per month by late 2012. This was at a time when the broader Bitcoin blockchain was experiencing hundreds of thousands of CoinJoin transactions monthly, as seen in Figure 2 of APPENDIX A.

Based solely on the government-provided Bitcoin Fog Addresses, these CoinJoins constituted only a small fraction of the overall CoinJoins on the Bitcoin blockchain, as demonstrated in Figure 4 of APPENDIX A. While the government concedes that its experts' heuristics almost certainly undercount the number of Bitcoin Fog Addresses, the prevalence of CoinJoins even before the advent of Bitcoin Fog makes it nearly impossible to quantify the extent of that undercounting, even at present.

More importantly, there is no observable increase in CoinJoins after the launch of Bitcoin Fog, unlike the significant uptick observed after Silk Road's launch in February 2011, as depicted in Figure 5 of APPENDIX A. It is reasonable to conclude that any undercounting of Bitcoin Fog Addresses is likely minimal at best, suggesting that Bitcoin Fog was merely one of many services generating CoinJoins, many of which were likely for individual use and remain largely unknown even today.

H. Overwhelming Prevalence of CoinJoins Undermines Reliability of Heuristics

It is evident that CoinJoins have existed since the Bitcoin blockchain's inception, and their use grew dramatically from 2009 through 2012. While the launch of Silk Road coincided with a significant increase in CoinJoin transactions,

the launches of both Bitcoin Fog and Mt. Gox did not materially increase CoinJoin use.

At best, Bitcoin Fog was responsible for only an insignificant fraction of all CoinJoins on the Bitcoin blockchain during its first year of operation. In 2012, the government's alleged Bitcoin Fog Addresses were involved in 21,450 CoinJoins out of a total of 14,982,632. This stark disparity clearly demonstrates that very little is known about CoinJoins during this critical period, significantly undermining the reliability of any heuristics applied to Bitcoin blockchain transactions from this era.

III. The Government Experts' Application of Their Experts' Heuristics was Flawed

The government's application of its flawed heuristics in this case casts doubt on the government's attribution claims, particularly regarding alleged early transactions related to Bitcoin Fog.

A key factor relied on by the government's expert was a transfer of bitcoin from a Mt. Gox exchange account to Bitcoin Fog's first mixing transaction via a Bitcoin address created before Bitcoin Fog's public launch ("Pre-Bitcoin Fog Transaction"). The government presented this transaction as evidence that the owner of the Mt. Gox exchange account knew about Bitcoin Fog as a service before it was launched, forming a critical part of their case that this owner created the Bitcoin Fog service.

However, the government expert's heuristics applied to the Pre-Bitcoin Fog Transaction must be rigorously analyzed against the widespread prevalence of CoinJoins on the Bitcoin blockchain at the time these transactions occurred. This analysis is essential to determine whether attributing the Pre-Bitcoin Fog Transaction to the owner of the Mt. Gox account is scientifically defensible. The government's expert testified:

Those addresses received funds in transactions 1, 2 and 4 here. And ultimately, the Bitcoin came out this address here, starting with – it is a little small. If we scroll up a bit more, we can see the Bitcoin originated in Mr. Sterlingov's plasma@plasmadivision Mt. Gox account. Funds were withdrawn from Mr. Sterlingov's Mt. Gox account, moved through a series of unusual transactions and were deposited into addresses I assessed are Bitcoin Fog deposit addresses prior to the announcement of Bitcoin Fog on Bitcoin Talk and Twitter

This tracing has been reproduced in Figure 1 of APPENDIX A, with additional annotations, describing the same flows and network as the government's Exhibit 317. Two specific aspects of the government expert's testimony warrant further scrutiny: first, the description of the transactions in Group A of Figure 1 as "unusual"; and second, the assertion of common ownership between the two transaction groups (Group A and Group B).

The government expert's opinion that Group A and Group B belong to the same person originates from their heuristics-based tracing methodologies, specifically the "co-spending" and "behavioral" heuristics. However, an analysis

of this tracing methodology, in the context of empirical CoinJoin analysis on the Bitcoin blockchain at the time, casts doubt regarding the reliability of such attribution.

I. The "Unusual" Transactions in Group A

The government's expert described the transactions in Group A as "unusual," likely because they were unaware that approximately 1 out of 3 of all Bitcoin blockchain transactions during that quarter were CoinJoins. If one operates under the mistaken assumption that CoinJoins were rare, then the transactions in Group A might indeed appear "unusual".

However, given the endemic nature of CoinJoins across the Bitcoin blockchain at the time these transactions occurred, and for several quarters prior, the transactions in Group A were not "unusual" in any meaningful sense, especially with respect to the empirical data reflected by the public Bitcoin blockchain ledger at that time.

J. No Reasonable Basis for Assuming Common Ownership

Referring to Figure 1 of APPENDIX A, the government's expert attributes common ownership to the 1NeW Bitcoin blockchain address and the 1M3n Bitcoin blockchain address, a conclusion drawn from a single bitcoin transfer with no other connections. No data is presented supporting this attribution for two Bitcoin blockchain addresses that could very simply be nothing more than counterparties.

Even applying the government expert's own "behavioral heuristic," there are clearly observable behavioral differences between the transactions in Group A and Group B. For instance, Group A's transactions consistently leave small amounts of unspent bitcoin behind in intermediary Bitcoin blockchain addresses, which remain unspent to this day. In stark contrast, Group B's transactions leave no such unspent amounts, instead feeding all transaction outputs directly to Bitcoin Fog.

Applying the government expert's own "behavioral heuristic" would imply that the 1NeW and 1M3n Bitcoin blockchain addresses would have different owners. Yet, the government's expert has reached a different conclusion based on the very same heuristic. This inconsistency in applying the same heuristic to two identical sets of blockchain transactions is precisely why the reliability of such methodologies demands a higher degree of scientific rigor than has been presented.

K. High False Negative Rate Disregarded by Government

Neither the government nor its experts presented blockchain analysis from any company other than Chainalysis Inc. The Scholl Report, in particular, explicitly refers to the use of Chainalysis Reactor software:

Based on the undercover transactions, five Bitcoin addresses can be attributed to BITCOIN FOG. Chainalysis Reactor attributed four of these five Bitcoin addresses to the BITCOIN FOG CLUSTER. Chainalysis Reactor did not cluster the fifth known address, BITCOIN FOG WITHDRAWAL ADDRESS 3,

however it did cluster the address which sent funds to BITCOIN FOG WITHDRAWAL ADDRESS 3.

Chainalysis Reactor did not include any of the addresses controlled by the government employees in the BITCOIN FOG CLUSTER. In other words, there were no false positives.

While it may be true that Chainalysis Reactor did not result in any "false positives" within this narrow dataset, neither the government nor its blockchain analysis considered "false negatives". Furthermore, no proof of the statistical resilience of its blockchain analysis was provided. Both "false positives" and "false negatives" are crucial statistical tests for determining error rates for given heuristics.

The Scholl Report's[24] failure to detect any "false positives" simply means that Chainalysis Reactor did not misidentify the government's undercover addresses as Bitcoin Fog for that specific and limited dataset. However, the report entirely disregards the significant "false negatives," where Chainalysis Reactor failed to identify 20% of the Bitcoin Fog addresses that the government itself had identified. A "false negative" rate of 20% is a high error rate. By comparison, the "false negative" rate for forensic latent fingerprint decisions

[24] Appx. 6400-64.

analyzed by the Proceedings of the National Academy of Sciences was found to be only 7.5%.[25]

One "false positive" rate and one "false negative" rate in a small study is definitively insufficient to determine the reliability of the heuristics being used.

IV. The Government Experts' Blockchain Analysis

The government's experts' blockchain analysis, while plausible in concept, is entirely devoid of the empirical rigor necessary for forensic evidence, thereby potentially invalidating its conclusions.

The heuristics employed by the government's experts are intuitively appealing. However, as the adage goes, "a broken clock tells the time correctly twice a day". Without empirical analysis, applying these heuristics and declaring them "very reliable" merely on the basis that they were occasionally correct, and without addressing the possibility of false positives and negatives, falls far short of the role of forensic evidence in the legal system.

The heuristics presented by the government's experts appear to have a statistically significant error rate. While a detective might accept a high error rate when searching for leads, the standard of evidence required for a lead is undeniably not the standard for its inclusion in evidence.

Consider a detective investigating a murder: the goal is to find the murderer among many leads. The detective's job is to investigate each lead to find the

[25] https://www.pnas.org/doi/full/10.1073/pnas.1018707108

murderer and corroborate the evidence. However, low true positive rates are far less useful when it comes to presenting evidence of who committed a crime. If, after investigating several suspects, one is found to have merely been in the same city as the crime, this is surely insufficient for a conclusion. The USNAS Report directly considers these issues and concludes:

> Finally, if evidence and laboratory tests are mishandled or improperly analyzed; if the scientific evidence carries a false sense of significance; or if there is bias, incompetence, or a lack of adequate internal controls for the evidence introduced by the forensic scientists and their laboratories, the jury or court can be misled, and this could lead to wrongful conviction or exoneration. If juries lose confidence in the reliability of forensic testimony, valid evidence might be discounted, and some innocent persons might be convicted or guilty individuals acquitted.

Given the overwhelming prevalence of CoinJoins on the Bitcoin blockchain at the time of the Appellant's alleged transactions, the blockchain analysis presented by the government's experts and reproduced in Figure 1 of APPENDIX A has done little more than establish that the Defendant was a Mt. Gox user at the time Bitcoin Fog was launched and made withdrawals. Much of the remaining blockchain analysis, however, possesses little forensic evidentiary value. Reliance on a flawed heuristic or fundamentally misunderstanding its evidentiary value thus opens itself to widespread abuse.

L. Limits to Blockchain Analysis

Blockchain analysis, as applied by the government's experts, is not entirely without merit but is of limited value.

First, the transactions under consideration occurred when the Bitcoin blockchain was relatively nascent. There is simply insufficient data about the parties transacting on the Bitcoin blockchain during that period, as evidenced by the government's own experts' conspicuous lack of information on CoinJoin prevalence.

Second, a multitude of transactions during that period generated significant "background noise". The price of bitcoin was relatively low, meaning transaction fees were also low, creating no real economic disincentives for engaging in multiple transactions to obfuscate sources or conduct multiple CoinJoins to ensure transactional privacy.

Third, neither the government nor its experts produced any corroborating evidence, such as servers or logs, that could have validated the blockchain analysis. In fact, the government appears to have relied heavily on blockchain analysis in a situation where such analysis would have been particularly unreliable.

The government's blockchain analysis is fundamentally flawed as a matter of forensic science and renders any data and results therefore unreliable. In addition, the basic evidentiary and statistical tests to verify the reliability of the blockchain analysis relied upon by the government and its experts have been completely disregarded.

Finally, to the extent that the government's conclusions rely upon its experts' unreliable and unverified blockchain analysis, in our opinion, such conclusions would necessarily also be unreliable.

CONCLUSION

This Court faces critical questions about the admissibility and reliability standards for blockchain analysis evidence that will have far-reaching implications for the cryptocurrency industry and criminal justice system. The technical evidence presented in this case exemplifies systemic deficiencies in how blockchain tracing methodologies are evaluated and admitted in federal courts.

The blockchain analysis industry operates largely without the scientific rigor and peer review that characterizes established forensic disciplines. The "co-spending" and behavioral heuristics employed by commercial blockchain analysis companies have not undergone the empirical testing necessary to establish their accuracy rates, particularly in environments with widespread privacy-enhancing transactions like CoinJoins. Courts lack the technical expertise to evaluate these proprietary methodologies, creating a dangerous precedent where unvalidated techniques may be accepted as reliable forensic evidence.

The prevalence of CoinJoins and other privacy-preserving transactions during the early Bitcoin era fundamentally undermines the reliability of heuristic-based attribution methods. Our empirical analysis demonstrates that such

transactions were endemic rather than exceptional during the relevant time period, contradicting the foundational assumptions underlying current blockchain tracing approaches.

This Court should establish clear standards requiring that blockchain analysis methodologies demonstrate their reliability through peer-reviewed research, statistical validation, and transparent disclosure of error rates before admission as evidence in criminal cases. Such standards would protect constitutional rights while encouraging the development of more robust and scientifically sound blockchain forensics.

The cryptocurrency and blockchain technology sector require clear judicial guidance on evidentiary standards to ensure that legitimate technological innovation is not stifled by unreliable forensic methodologies. Courts must demand the same level of scientific rigor for blockchain evidence that has been established for other forms of technical evidence.

ChainArgos respectfully urges this Court to require that blockchain analysis evidence meet established standards for scientific reliability before admission, thereby protecting both constitutional rights and the integrity of an emerging technology sector that is vital to America's technological leadership.

Dated: September 22, 2025

Respectfully submitted,

/s/_____
Joseph A. Scrofano
Scrofano Law PC

D.C. Cir. Bar No: 60117
600 F St NW Suite 300
Washington, DC 20004
(202) 870-0889
jas@scrofanolaw.com

CERTIFICATE OF COMPLIANCE

This document complies with the type-volume and word-count limits of Fed. R. App. P. 29(a)(5) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f), this document contains 6,002 words. This document complies with the typeface and type-style requirements of Fed. R. App. P. 27(d) because this document has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman font.

/s/_____
Joseph A. Scrofano

CERTIFICATE OF SERVICE

I certify that I electronically filed the Motion for Leave to Participate as Amicus Curiae with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit using the appellate CM/ECF system on September 22, 2025. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF System.

/s/_____
Joseph A. Scrofano

APPENDIX A

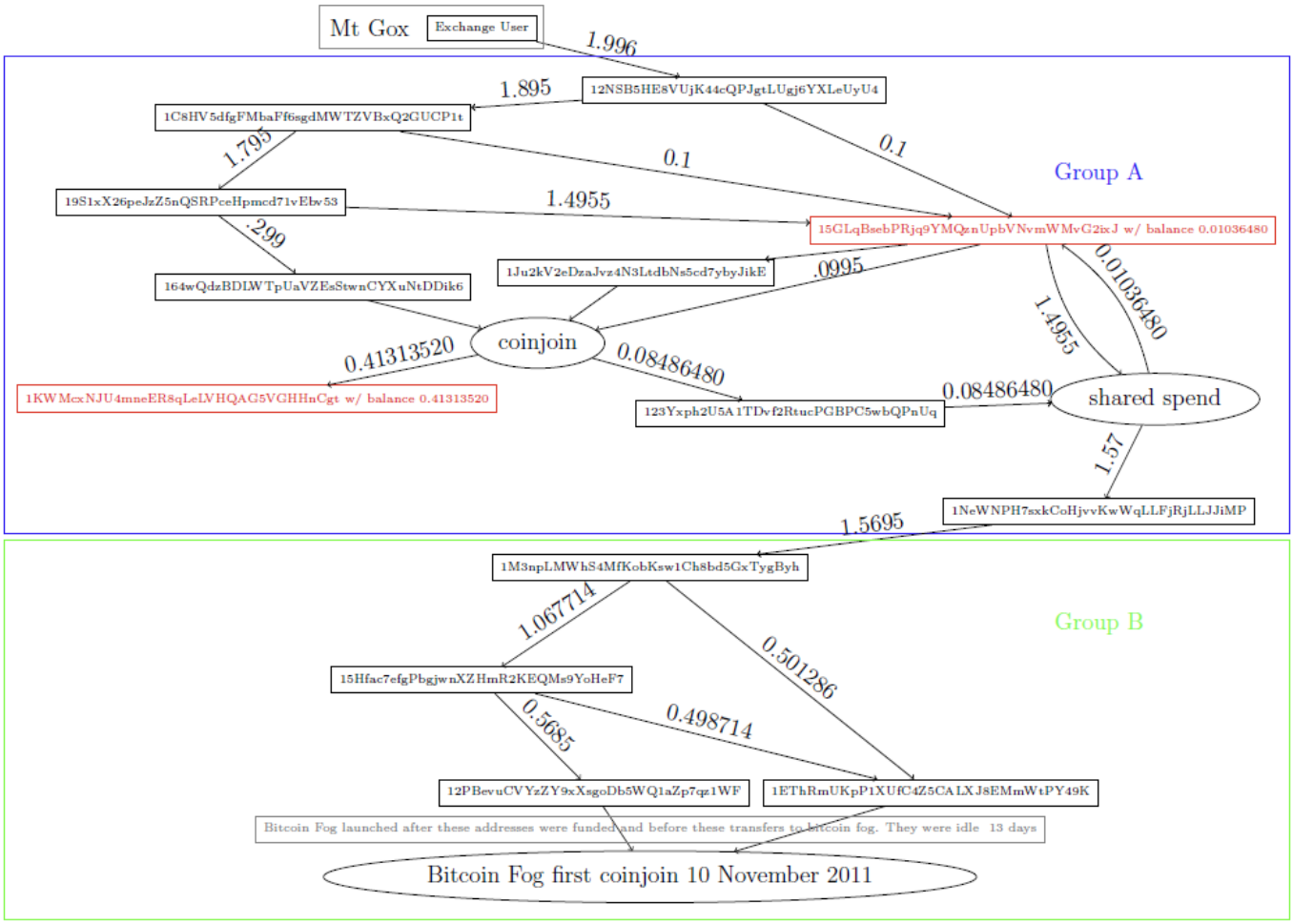

Figure 1: Pre-launch transactions attributed to Bitcoin Fog in. Bitcoin Fog's launch was announced on bitcointalk.org on 27 October 5:07PM EST.

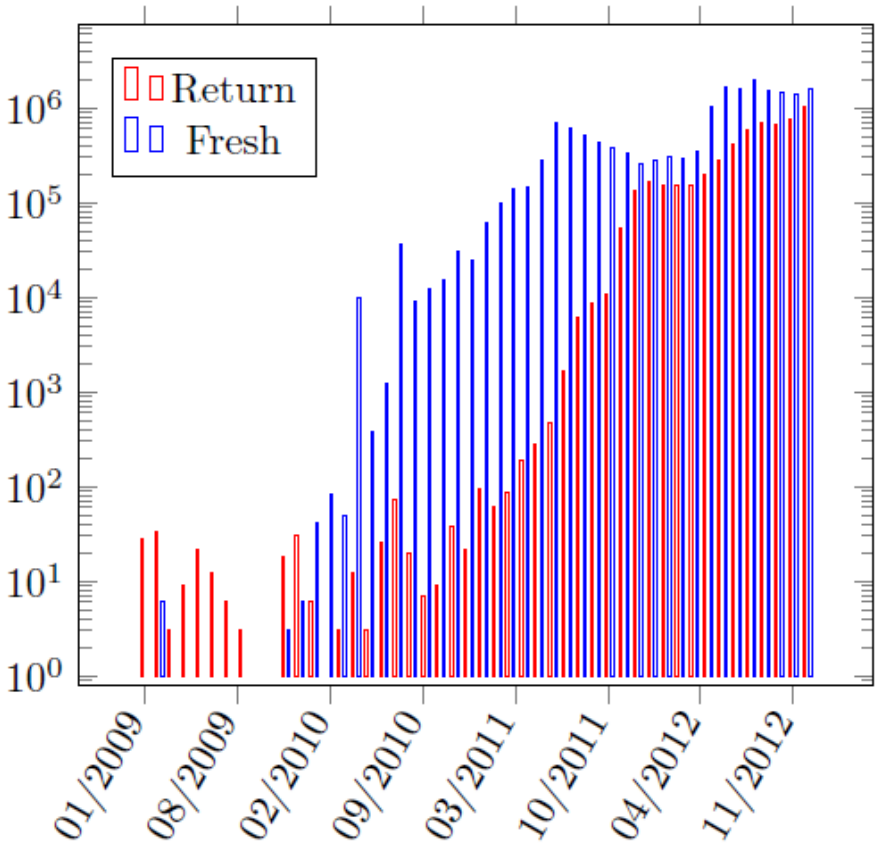

Figure 2: Monthly payment transactions where either change is returned to the sender (red) or sent to a fresh address (blue).

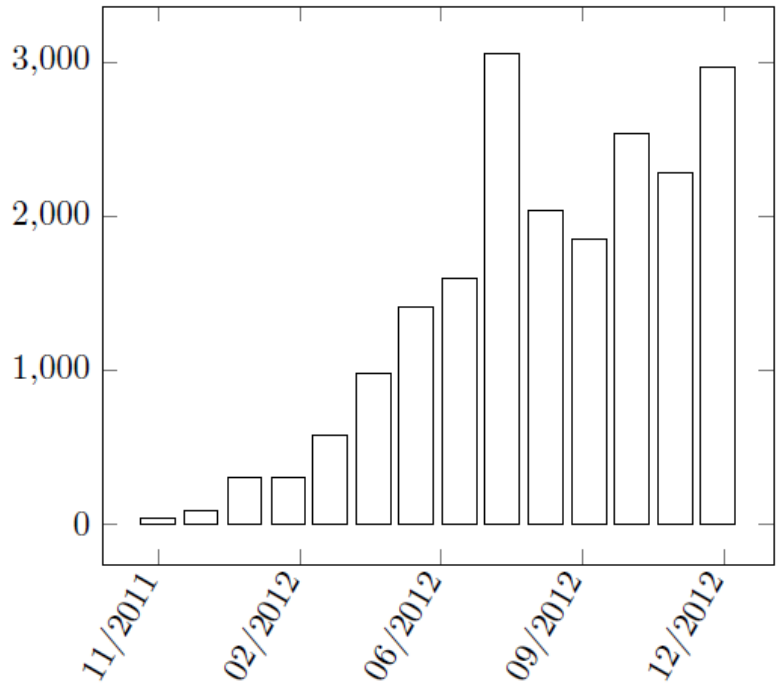

Figure 3: Bitcoin Fog Addresses CoinJoins per Month

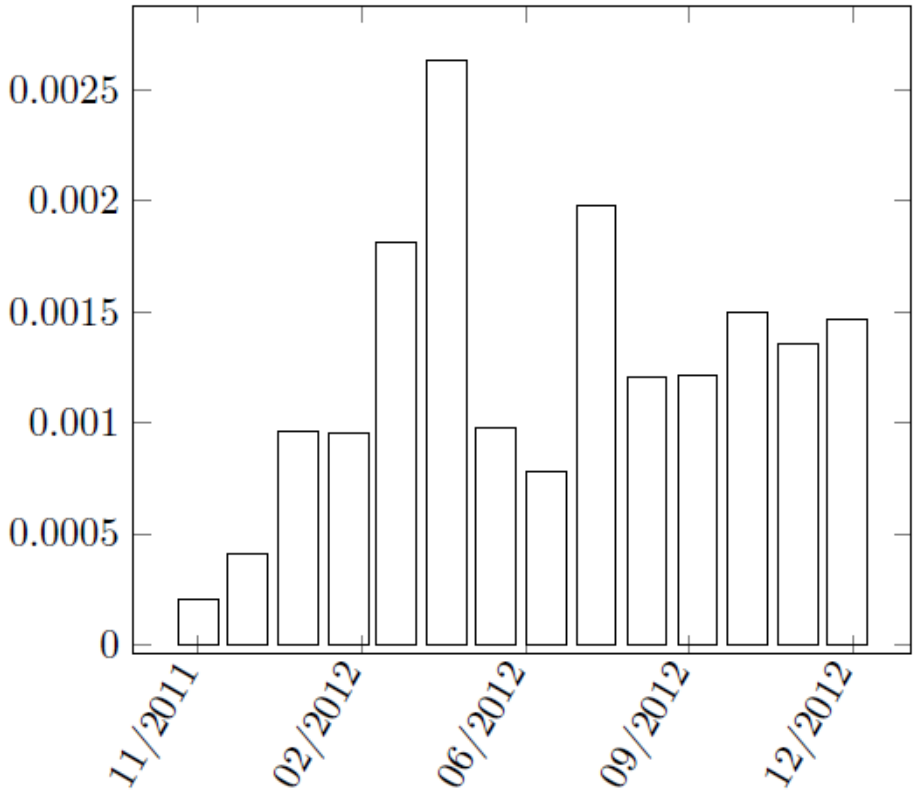

Figure 4: Percentage of all CoinJoins that involve Bitcoin Fog Addresses as provided by the government.

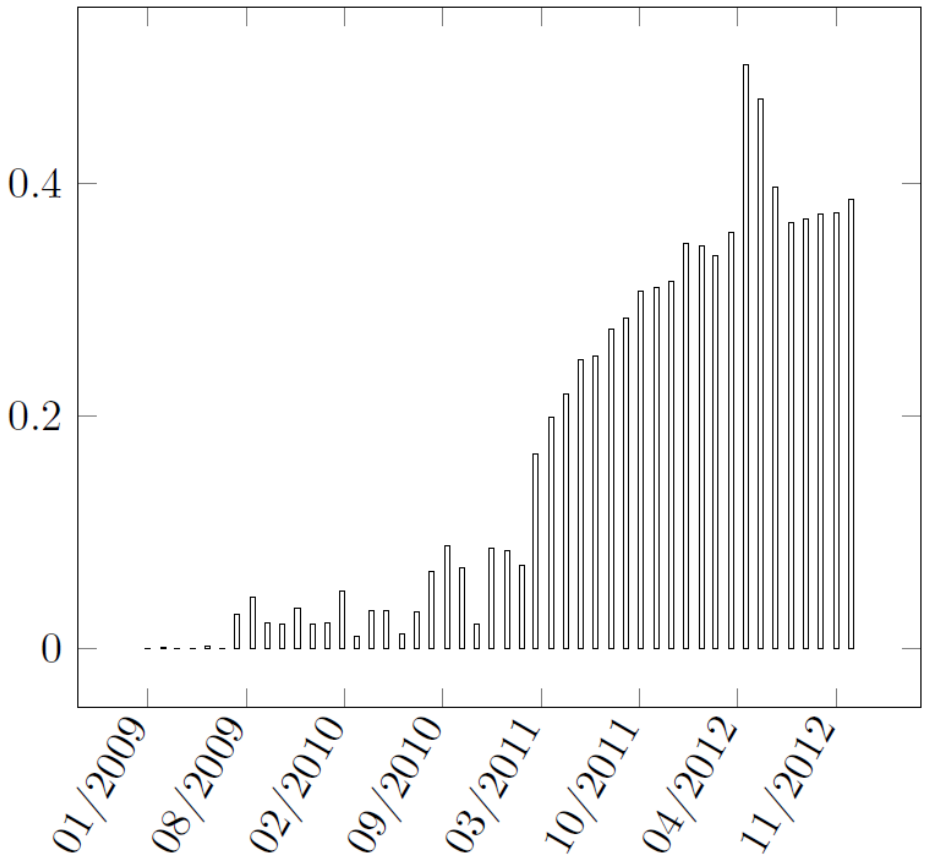

Figure 5: Fraction of all transactions in each month that are CoinJoins.